LAW OFFICES
GIFFORD, KRASS, GROH, SPRINKLE, ANDERSON & CITKOWSKI, P.C.
PATENT, TRADEMARK AND COPYRIGHT PRACTICE
101 N. MAIN STREET
SUITE 800
ANN ARBOR, MICHIGAN 48104-1476

(734) 913-9300
FACSIMILE (734) 913-6007
jposa@patlaw.com
dwathen@patlaw.com
mbancroft@patlaw.com
jstaple@patlaw.com

FACSIMILE TRANSMISSION

DATE: December 7, 2004

TO: EXAMINER LASHONDA JACOBS

FACSIMILE NO.: 703-872-9306

FROM: John G. Posa

PAGES TRANSMITTED (INCLUDING COVER SHEET): 3

ORIGINAL DOCUMENTS WILL _____ / WILL NOT ___X__ FOLLOW BY MAIL

RE: SN 09/877,596

MESSAGE:

Examiner Jacobs:

The attached document corresponds to the amendment and affidavit filed via facsimile on Dec. 3, 2004 for the above-referenced application. This document was stated as being an attachment to the affidavit; however, it was inadvertently missing from the papers filed Dec. 3, 2004.

RECEIVED
CENTRAL FAX CENTER
DEC 07 2004

Method for Secure Transactions Utilizing Physically Separated Computers

Field of the Invention

This invention relates to transactions conducted over computer networks, and, more particularly, to a system for securing transactions between physically separated participants from unauthorized users.

Background of the Invention

While the near-universal availability of the Internet to users in every location has created opportunities for many new kinds of businesses, it also has opened new opportunities for fraudulent use of credit card credentials by unscrupulous criminals. In these types of transactions (referred to as "card not present" transactions), the buyer of a product provides the seller with credit card information which cannot physically be verified, because the entire transaction occurs between remote participants and/or computers. Even in cases in which a customer service clerk speaks directly to the buyer to obtain the credit card information, there is no way to verify that the credit card credentials are legitimately obtained, or that the buyer is authorized to use the credentials to effect the transaction.

Various systems have been proposed or implemented in which the buyer is expected to provide information for verification, such as the maiden name of the buyer's mother, some form of biometric information, or a scan of the physical credit card through a remote reader in the buyer's computer. In each case, these types of data may be obtained through outside sources of information, simulated, or impersonated through computer means.

Summary of the Invention

In the instant invention, a method is disclosed by which verification of credentials may be accomplished using a separate, pre-established communications path. Whether the transaction is initiated by direct verbal contact or by computer communication over a wide-area communication network, such as the Internet, the credit card credentials are provided in the usual manner. After the credentials are recorded, the proposed transaction is forwarded to the credit card clearinghouse for authorization.

At this point, the credit card clearinghouse forwards a request for verification to an e-mail account which previously has been designated by the credit card holder. This could be an account maintained for the holder by the clearinghouse itself, or it could be an

independently maintained e-mail account at an "external" service provider. The request itself would carry sufficient information for the holder to identify the transaction items and the originating merchant; as a example, this would include information identifying the merchant, the items ordered, and the total amount requested to be approved. The holder then would be required to accept the transaction by acknowledging the contents of the e-mail message. If the user already is on-line with the merchant at the time of the transaction, it is a simple matter for the holder to open a new window in his or her "Browser" and retrieve this e-mail message. Current technology allows the use of various types of messaging "agents" which can provide near-immediate notification of the arrival of messages; another option would be to implement a wide-area communications protocol which would give priority to the carriage of certain types of transactional information and messages. In addition, software can be incorporated into the Browser application by which certain types of pre-configured communications links could be implemented with a single click of a computer "mouse".

For verbal orders, or in the case that the credit card holder cannot retrieve the e-mail message immediately, the holder would have a pre-determined period of time in which to perform the verification of the e-mail (for example, 12 hours) after which the transaction automatically would be canceled.

In an alternative embodiment, an "external" e-mail account could be programmed to automatically respond to a specific e-mail message by generating a reply message to be sent to the clearinghouse, similar to the manner in which e-mail systems automatically handle "spam" messages from identified senders. It also could respond by sending a message specific to the transaction that has been prepared in advance by the holder, in anticipation of the confirmation request from the clearinghouse.

A further enhancement would be to employ encryption to the various messages and responses, to ensure that only the credit card holder can access and respond to the messages. This encryption system could include the transmission and decoding of a specialized information file, which, among other things, could include information specific to the transaction (such as a transaction identifier or merchant number), or might require combination with additional information which would be provided by the holder. An alternative embodiment might include the application of an algorithm specific to the holder or to the transaction to modify existing data or to create new data as part of the verification method.

As an added benefit, the existence of routing information attached to the transmitted or returned messages would allow verification of the source computer for the response message, as well as providing an "audit trail" for the entire transaction.